SENIOR USER

(Please circle the appropriate status for each measure)

PROTECTIVE MEASURE	STATUS				
Users have been instructed that certain types of unclassified information require protection and have been told how to identify these types of information.	I	P	AR	NA	DK
All sensitive storage media, to include computer listings, are labeled with an appropriate safeguard statement.	I	P	AR	NA	DK
All removable media is labeled with the information owner's name, date of creation, identification of contents and control number.	I	P	AR	NA	DK
Prior to entering information on a system, users determine the sensitivity level of information and verify that the system is authorized to handle that level of information.	I	P	AR	NA	DK
Users protect inputs and outputs from casual observation.	I	P	AR	NA	DK
Users direct sensitive files to remote devices only when the remote device is known to be in a secure area and staffed by authorized persons.	I	P	AR	NA	DK
Procedures are in place to insure that ordinary trash does not contain sensitive information.	I	P	AR	NA	DK
Users are trained in how to establish the value of information.	I	P	AR	NA	DK
Before leaving a work area unattended, users lock all sensitive information, in physical form, in a container which cannot be removed easily from the work area.	I	P	AR	NA	DK

Key I=Implemented, P=Planned, AR=Accepting Risk; NA=Not Applicable, and DK=Don’t Know

SENIOR USER

(Please circle the appropriate status for each measure)

PROTECTIVE MEASURE	STATUS
Users properly discard of all sensitive waste, to include media which contain latent impressions such as typewriter ribbons.	I P AR NA DK
Users decide what file protections are appropriate for their files based on the sensitivity level of the information in the files.	I P AR NA DK
File sharing rules, including group identifiers, are reviewed by users at least annually.	I P AR NA DK
Users are required to change their passwords at least once every six months.	I P AR NA DK
Users are instructed not to share, write down or electronically store passwords.	I P AR NA DK
Users are instructed to immediately change passwords they suspect of being compromised.	I P AR NA DK
Users are instructed not to log onto systems for other individuals.	I P AR NA DK
Users sign a statement acknowledging they are aware of the proper procedures for selecting and protecting passwords.	I P AR NA DK
Users are instructed not to sign on to more than one remote terminal/workstation at a time unless they can keep all such terminals/workstations under constant surveillance.	I P AR NA DK
Users are instructed to log off remote terminals/workstations when leaving them unattended, except that software locking devices may be used when the terminal will be unattended for less than 30 minutes.	I P AR NA DK

Key I=Implemented, P=Planned, AR=Accepting Risk; NA=Not Applicable, and DK=Don’t Know

SENIOR ADMINISTRATOR

(Please circle the appropriate status for each measure)

PROTECTIVE MEASURE	STATUS				
Data and document retention procedures are sufficiently complete to ensure adequate capability to restore critical data and applications systems.	I	P	AR	NA	DK
Systems and operations persons are thoroughly trained in restart and recovery procedures.	I	P	AR	NA	DK
Documentation for the restart/recovery process is complete, understandable and readily available.	I	P	AR	NA	DK
Procedures are in place to insure that a system crash will not leave sensitive information unprotected.	I	P	AR	NA	DK
There is an individual in the organization with expertise in the technical aspects of recovery, dump and restore, unloading/reloading of data and transaction and program checkpointing.	I	P	AR	NA	DK
Known system vulnerabilities associated with checkpoint/restart and use of recovery utilities have been identified and corrected were possible.	I	P	AR	NA	DK
The data recovery system protects against user program failure and system failure.	I	P	AR	NA	DK
System dumps are always taken after a system crash	I	P	AR	NA	DK
All output, to include system dumps and source listings, which contains sensitive information is controlled.	I	P	AR	NA	DK

Key I=Implemented, P=Planned, AR=Accepting Risk; NA=Not Applicable, and DK=Don’t Know

SENIOR ADMINISTRATOR

(Please circle the appropriate status for each measure)

PROTECTIVE MEASURE	STATUS				
System administrators insure listings they produce never contain any information which could facilitate unauthorized access to the system, such as passwords.	I	P	AR	NA	DK
System administrators have been trained to implement the security features of the operating system which they use.	I	P	AR	NA	DK
For terminating/transferring employees, the system administrator cancels passwords and entries in authorization tables, and passes ownership to his replacement for on-line files, etc..	I	P	AR	NA	DK
The system administrator (within 48 hours) deletes a person's password when notified that the person no longer is authorized access to the system.	I	P	AR	NA	DK
Access from remote machines, without password validation, is permitted only when acceptable security standards are known to exist on those remote machines.	I	P	AR	NA	DK
All userids are known to the system administrator.	I	P	AR	NA	DK
The system administrator occasionally tests the system to see if it is possible to sign on with a valid user name and password combination from an unauthorized remote device.	I	P	AR	NA	DK
A complete system backup is accomplished at least monthly.	I	P	AR	NA	DK
Changed data files are backed up at least weekly.	I	P	AR	NA	DK

Key I=Implemented, P=Planned, AR=Accepting Risk; NA=Not Applicable, and DK=Don't Know

SENIOR ADMINISTRATOR

(Please circle the appropriate status for each measure)

PROTECTIVE MEASURE	STATUS				
The retention period for backed up data has been coordinated with the users.	I	P	AR	NA	DK
At least two generations of back ups are available, with the oldest being stored in a location not in the immediate vicinity of the system.	I	P	AR	NA	DK
Tests have been conducted to insure that backups can be relied upon.	I	P	AR	NA	DK
The entire system is backed up at least once a week.	I	P	AR	NA	DK
Changed data files are backed up daily.	I	P	AR	NA	DK
All magnetic media containing sensitive information is stored in metal or other fire retardant cabinets.	I	P	AR	NA	DK
Preventive maintenance of all hardware is accomplished in accordance with vendor prescribed schedules.	I	P	AR	NA	DK
Power surge protection is provided for all system hardware.	I	P	AR	NA	DK
Standard procedures are used for configuring hardware.	I	P	AR	NA	DK
All areas containing system equipment have sufficient heating, ventilation and air conditioning systems to maintain an appropriate temperature/humidity range.	I	P	AR	NA	DK
System software documentation is complete and stored in a secure location.	I	P	AR	NA	DK

Key I=Implemented, P=Planned, AR=Accepting Risk; NA=Not Applicable, and DK=Don’t Know

SENIOR ADMINISTRATOR

(Please circle the appropriate status for each measure)

PROTECTIVE MEASURE	STATUS
Standard procedures are used for configuring system software.	I P AR NA DK
Procedures exist to test new operating system releases prior to using them in production.	I P AR NA DK
Imported software is installed on the system only after the software has been reasonably determined to be safe for use in its intended environment.	I P AR NA DK

Key I=Implemented, P=Planned, AR=Accepting Risk; NA=Not Applicable, and DK=Don’t Know

BUILDING COORDINATOR

(Please circle the appropriate status for each measure)

PROTECTIVE MEASURE	STATUS
Water detectors are located under raised floors.	I P AR NA DK
If the facility has outside windows, the glass has been replaced by reinforced panes or otherwise protected by external screens.	I P AR NA DK
The facility operations manager (FOM) is aware of his/her responsibilities for the physical security of the building as discussed in applicable NASA Security Handbooks.	I P AR NA DK
After normal business hours, all windows and doors to the building are locked to prevent access from the outside.	I P AR NA DK
Keys to building entrance doors are controlled.	I P AR NA DK
All entrances to the building are well lighted during hours of darkness.	I P AR NA DK
The site security force routinely checks the exterior security of the building after normal business hours.	I P AR NA DK
Visitors and employees are required to display their security badges while in the building.	I P AR NA DK
The facility operations manager (FOM) is responsible for insuring there is adequate fire protection for the building.	I P AR NA DK
Sufficient electrical circuits are available to preclude an overload situation.	I P AR NA DK

Key I=Implemented, P=Planned, AR=Accepting Risk; NA=Not Applicable, and DK=Don’t Know

BUILDING COORDINATOR

(Please circle the appropriate status for each measure)

PROTECTIVE MEASURE	STATUS				
There are appropriate alarm systems for fire and smoke.	I	P	AR	NA	DK
Fire drills are conducted on a regular basis.	I	P	AR	NA	DK
Adequate emergency exits are available in the event of fire.	I	P	AR	NA	DK
Fire detection devices, such as smoke or heat-rise detectors, are installed in the overhead areas and beneath raised floors.	I	P	AR	NA	DK
The facility is equipped with control panels that monitor smoke detectors indicating their operational status.	I	P	AR	NA	DK
All switches, control panels and circuit breaker panels are labeled to indicate the outlets/equipment they support.	I	P	AR	NA	DK

Key I=Implemented, P=Planned, AR=Accepting Risk; NA=Not Applicable, and DK=Don’t Know

BRANCH REPRESENTATIVE

(Please circle the appropriate status for each measure)

PROTECTIVE MEASURE **STATUS**

PROPERTY CUSTODIAN

(Please circle the appropriate status for each measure)

PROTECTIVE MEASURE	STATUS				
Users sign NASA Form 1602 "NASA Equipment Management Systems (NEMS) Transaction Document" [November 1989] listing all equipment for which they have primary responsibility.	I	P	AR	NA	DK
A physical inventory of all system hardware is accomplished at least once a year.	I	P	AR	NA	DK
The property custodian conducts a physical inventory of all hardware listed on a user's Form 1602 "NASA Equipment Management Systems (NEMS) Transaction Document" [November 1989] prior to that user leaving the organization.	I	P	AR	NA	DK

KEY: I = Implemented; P = Planned; AR = Accepting Risk; NA = Not Applicable; DK = Don't Know

BRANCH REPRESENTATIVE

(Please circle the appropriate status for each measure)

PROTECTIVE MEASURE **STATUS**

UNIX USER

(Please circle the appropriate status for each measure)

PROTECTIVE MEASURE	STATUS				
UNIX users are presented a message at login warning that they are trying to access a Federal government computer which is to be used for official government purposes only.	I	P	AR	NA	DK
UNIX users must enter a valid userid and password combination to gain access to the system.	I	P	AR	NA	DK
UNIX systems insure that the response to an unsuccessful login does not give the details of valid user name and password characteristics.	I	P	AR	NA	DK
UNIX systems require that users select passwords that are at least six characters long.	I	P	AR	NA	DK
UNIX systems do not display passwords when entered.	I	P	AR	NA	DK
UNIX systems insure users change passwords at least once every six months.	I	P	AR	NA	DK
UNIX users are instructed not to share, write down or electronically store passwords.	I	P	AR	NA	DK
UNIX users are instructed to immediately change passwords they suspect of being compromised.	I	P	AR	NA	DK
UNIX users are instructed not to log onto systems for other individuals.	I	P	AR	NA	DK
UNIX users sign a statement acknowledging they are aware of the proper procedures for selecting and protecting passwords.	I	P	AR	NA	DK

KEY: I = Implemented; P = Planned; AR = Accepting Risk; NA = Not Applicable; DK = Don't Know

BRANCH REPRESENTATIVE

(Please circle the appropriate status for each measure)

PROTECTIVE MEASURE **STATUS**

UNIX USER

(Please circle the appropriate status for each measure)

PROTECTIVE MEASURE	STATUS				
UNIX users are instructed not to sign onto more than one remote terminal/workstation at a time unless they can keep all such terminals/workstations under constant surveillance.	I	P	AR	NA	DK
UNIX users are instructed to log off remote terminals/workstations when leaving them unattended, except that software locking devices may be used when the terminal will be unattended for less than 30 minutes.	I	P	AR	NA	DK
UNIX users have been instructed that certain types of unclassified information require protection and have been told how to identify these types of information.	I	P	AR	NA	DK
Procedures are in place to insure that ordinary trash does not contain sensitive information.	I	P	AR	NA	DK
Before leaving a work area unattended, users lock all sensitive information, in physical form, in a container which cannot be removed easily from the work area.	I	P	AR	NA	DK

KEY: I = Implemented; P = Planned; AR = Accepting Risk; NA = Not Applicable; DK = Don't Know

BRANCH REPRESENTATIVE

(Please circle the appropriate status for each measure)

PROTECTIVE MEASURE **STATUS**

UNIX ADMINISTRATOR

(Please circle the appropriate status for each measure)

PROTECTIVE MEASURE	STATUS				
The UNIX root account profile has a umask of 022 (rwxr-xr-x) at minimum.	I	P	AR	NA	DK
Individual UNIX account profiles have a umask of 027 (rwxr-x---) at minimum.	I	P	AR	NA	DK
The UNIX system wide default umask is not set to grant write to other.	I	P	AR	NA	DK
The UNIX system administrator uses groups for accounting purposes and for sharing data.	I	P	AR	NA	DK
The UNIX system administrator insures there are no setuid or setgid shell scripts on the system.	I	P	AR	NA	DK
The UNIX system administrator checks all "nonstandard" setuid and setgid programs for security.	I	P	AR	NA	DK
The UNIX system administrator insures that setuid bit is removed from /usr/etc/restore.	I	P	AR	NA	DK
The UNIX system administrator insures that sticky bits are set on all world-writable directories except /usr/tmp.	I	P	AR	NA	DK
The UNIX system administrator insures that proper modes are set on devices in /dev.	I	P	AR	NA	DK
The /etc/password file in UNIX is protected, at minimum, with permission of 770 (rwxrwx---).	I	P	AR	NA	DK
The /etc/shadow file in UNIX is protected, at a minimum, with permission of 770 (rwxrwx---).	I	P	AR	NA	DK
The /etc/profile file in UNIX is protected, at minimum, with permission of 775.	I	P	AR	NA	DK

KEY: I = Implemented; P = Planned; AR = Accepting Risk; NA = Not Applicable; DK = Don't Know

BRANCH REPRESENTATIVE

(Please circle the appropriate status for each measure)

PROTECTIVE MEASURE **STATUS**

UNIX ADMINISTRATOR

(Please circle the appropriate status for each measure)

PROTECTIVE MEASURE	STATUS				
The UNIX system administrator reviews sulog reports at least weekly.	I	P	AR	NA	DK
The UNIX system administrator reviews the pacct and wtmp reports at least weekly.	I	P	AR	NA	DK
The UNIX system administrator insures that pacct and wtmp files are protected against world write.	I	P	AR	NA	DK
The UNIX system administrator insures all vendor embedded passwords are removed immediately after they are no longer needed.	I	P	AR	NA	DK
The UNIX system administrator insures that no accounts, such as group accounts, share passwords among users.	I	P	AR	NA	DK
If running the network file system (NFS), UNIX system administrators insure that all lines in the password or group file which should have a "+" the first space on the line do, in fact, have a "+" present.	I	P	AR	NA	DK
The UNIX system administrator insures that guest accounts which are no longer needed are removed.	I	P	AR	NA	DK
The UNIX system administrator uses an automated tool, such as CRACK, to determine if users have easily guessable passwords.	I	P	AR	NA	DK
The UNIX system administrator insures that the response to an unsuccessful login displayed on the monitor does not give the details of valid user name and password characteristics. [This is standard on most UNIX-like systems.]	I	P	AR	NA	DK

KEY: I = Implemented; P = Planned; AR = Accepting Risk; NA = Not Applicable; DK = Don't Know

BRANCH REPRESENTATIVE

(Please circle the appropriate status for each measure)

PROTECTIVE MEASURE **STATUS**

UNIX ADMINISTRATOR

(Please circle the appropriate status for each measure)

PROTECTIVE MEASURE	STATUS				
The UNIX system administrator occassionally checks user .netrc files to insure they do not contain clear text passwords.	I	P	AR	NA	DK
The system requires UNIX users to enter a valid user name and password combination prior to being granted access. [This is a standard feature of UNIX-like systems.]	I	P	AR	NA	DK
The system forces UNIX users to change temporary passwords the first time they login using that password.	I	P	AR	NA	DK
All on-line records of passwords are either encrypted or accessible only to individuals with UNIX system administrator privileges.	I	P	AR	NA	DK
The UNIX operating system, or a suitable utility, insures that passwords are not readable when entered on input devices. [Ordinarily, this is a standard feature on UNIX-like systems]	I	P	AR	NA	DK
A password aging utility insures users change passwords for UNIX systems at least once every six months.	I	P	AR	NA	DK
The UNIX operating system, or a suitable utility, enforces an expiration date on all accounts.	I	P	AR	NA	DK
All UNIX accounts have passwords or "*" in the password field of /etc/passwd and /etc/shadow/passwd.	I	P	AR	NA	DK
The UNIX operating system, or a suitable utility, requires that all passwords contain at least six alphanumeric characters and at least one non-alphanumeric character.	I	P	AR	NA	DK

KEY: I = Implemented; P = Planned; AR = Accepting Risk; NA = Not Applicable; DK = Don't Know

BRANCH REPRESENTATIVE

(Please circle the appropriate status for each measure)

PROTECTIVE MEASURE **STATUS**

UNIX ADMINISTRATOR

(Please circle the appropriate status for each measure)

PROTECTIVE MEASURE	STATUS
The UNIX operating system, or a suitable utility, forces users to change temporary passwords the first time they login using that password.	I P AR NA DK
Users are presented a message at login warning them that they have accessed a Federal government computer which is to be used for official government purposes only.	I P AR NA DK
The UNIX operating system, or a suitable utility, insures passwords are not reused within a one year period.	I P AR NA DK
The UNIX system administrator insures the hosts.equiv file contains only local organizational hosts and no "+".	I P AR NA DK
The UNIX system administrator insures only "console" is labeled as "secure" in ttytab, and only if the console is a server located in a restricted area.	I P AR NA DK
The UNIX system administrator insures no terminals are labeled as "secure" in ttytab (clients only).	I P AR NA DK
No UNIX network file systems (NFS) are exported to the world.	I P AR NA DK
The UNIX system administrator insures that the system's version of ftpd is dated later than December 1988.	I P AR NA DK
The UNIX system administrator insures there is no "decode" alias in the aliases file.	I P AR NA DK
The UNIX system administrator insures there is no "wizard" password in sendmail.cf.	I P AR NA DK

KEY: I = Implemented; P = Planned; AR = Accepting Risk; NA = Not Applicable; DK = Don't Know

BRANCH REPRESENTATIVE

(Please circle the appropriate status for each measure)

PROTECTIVE MEASURE **STATUS**

UNIX ADMINISTRATOR

(Please circle the appropriate status for each measure)

PROTECTIVE MEASURE	STATUS
The UNIX system administrator insures there is no "debug" command in sendmail.	I P AR NA DK
The UNIX system administrator insures the version of fingerd is dated later than November 5, 1988.	I P AR NA DK
The UNIX system administrator insures that modems and terminal servers handle hangups correctly.	I P AR NA DK
The UNIX system administrator 'spot checks' users' .forward files to insure they are accessible by the owner only.	I P AR NA DK
Site personnel are informed of how to report known or suspected unauthorized access to the site.	I P AR NA DK
All systems included in this assessment are contained in buildings enclosed by perimeter fencing.	I P AR NA DK
All systems are contained within a perimeter where site entry control points are continually guarded or securely locked at all times.	I P AR NA DK
All systems are located within a perimeter where, under normal security conditions, vehicles are checked for authorized decals prior to being allowed to enter.	I P AR NA DK
All systems are within a perimeter where vehicles without decals are stopped and, after verification of a legitimate need to enter, a temporary vehicle pass is issued.	I P AR NA DK
All systems are within a perimeter where all employees and on-site contractors are issued a security badges.	I P AR NA DK

KEY: I = Implemented; P = Planned; AR = Accepting Risk; NA = Not Applicable; DK = Don't Know

BRANCH REPRESENTATIVE

(Please circle the appropriate status for each measure)

PROTECTIVE MEASURE	STATUS
Water proof sheets are available for covering equipment in an emergency water protection situation.	I P AR NA DK
The location of plumbing cut offs are known by supervisors so they can be shut off quickly in emergencies.	I P AR NA DK
The operations and equipment installations, programmer offices and data files are located above the ground floor.	I P AR NA DK
Line management insures that an owner is identified for all sensitive information stored in physical form.	I P AR NA DK
All persons receive an initial orientation in automated information security basics prior to being allowed to use systems belonging to the organization.	I P AR NA DK
All persons sign a statement acknowledging their responsibilities with respect to automated information security prior to being issued a password for any system in the organization.	I P AR NA DK
All persons are trained in how to report an actual or suspected security violation.	I P AR NA DK
Line managers are trained in how to use NHB 2410.9 to develop effective AIS policies and procedures for their organization.	I P AR NA DK
Procedures have been established to insure that users at remote processing sites are informed of their responsibilities for automated infomation security.	I P AR NA DK
All persons are instructed in how to select and secure passwords prior to being authorized access to any system in the organization.	I P AR NA DK
All persons receive special training in handling sensitive information prior to being to being allowed to handle any sensitive information.	I P AR NA DK
All persons involved in remote processing are trained in the security aspects of using networks, remote file servers, and remote printing devices.	I P AR NA DK

KEY: I = Implemented; P = Planned; AR = Accepting Risk; NA = Not Applicable; DK = Don't Know

BRANCH REPRESENTATIVE

(Please circle the appropriate status for each measure)

PROTECTIVE MEASURE	STATUS				
Line managers are provided special training in implementing effective risk management programs.	I	P	AR	NA	DK
Line managers are provided special training in developing overall AIS plans.	I	P	AR	NA	DK
Inexperienced employees are closely supervised and constrained from working alone. .	I	P	AR	NA	DK
All employees demonstrate a satisfactory level of competence on each automated information system prior to being allowed to use the system without supervision.	I	P	AR	NA	DK
Users receive on-the-job and/or formal training on specific hardware devices prior to allowing them to use these devices.	I	P	AR	NA	DK
Users receive on-the-job and/or formal training on automated applications, the operating system, and software handling procedures prior to allowing them to use an automated system.	I	P	AR	NA	DK
Users receive special training when there are major changes to the automated information systems which they use.	I	P	AR	NA	DK
Users receive on-the-job and/or formal training in electronic file management and transfer.	I	P	AR	NA	DK
System administrators receive on-the-job and/or formal training on the operating system they use.	I	P	AR	NA	DK
Site personnel are informed of how to report known or suspected unauthorized access to sensitive information.	I	P	AR	NA	DK
Line management has established procedures to insure that sensitive information, in physical form, is released only to individuals authorized by the information owner.	I	P	AR	NA	DK
Site personnel have been instructed to insure, when possible, that sensitive material is removed from hardware devices prior	I	P	AR	NA	DK

KEY: I = Implemented; P = Planned; AR = Accepting Risk; NA = Not Applicable; DK = Don't Know

BRANCH REPRESENTATIVE

(Please circle the appropriate status for each measure)

PROTECTIVE MEASURE	STATUS
to those devices receiving maintenance services.	
When sensitive material cannot be removed from devices prior to maintenance, maintenance personnel are properly screened or are closely supervised by someone who is.	I P AR NA DK
Line management enforces a policy that, at the end of the work day, sensitive information is removed from all systems which are not password protected or protected by a physical locking device.	I P AR NA DK
Lock combinations to cabinets containing sensitive information are changed periodically and whenever key persons leave the organization.	I P AR NA DK
Sensitive information (including copyrighted software) is removed from hardware devices prior to transferring ownership of those devices unless the information/software is specifically included in the transfer. [This includes PCs & Macs.]	I P AR NA DK
It is organization policy that an owner be identified for all files on all systems in the organization.	I P AR NA DK
The organization enforces a policy of not using anonymous FTP to transmit files containing sensitive information.	I P AR NA DK
The organization head insures a code of ethics exists which defines acceptable standards of conduct for employees using the organization's automated information systems.	I P AR NA DK
The supervisor of a terminating/transferring employee immediately notifies the system administrator for all systems to which the employee had access.	I P AR NA DK
Supervisors are alert for employee emotional instability, alcoholism, drug abuse and financial insolvency.	I P AR NA DK
All new employees are informed of the organization's ethical standards and their responsibility to abide by them.	I P AR NA DK

KEY: I = Implemented; P = Planned; AR = Accepting Risk; NA = Not Applicable; DK = Don't Know

BRANCH REPRESENTATIVE

(Please circle the appropriate status for each measure)

PROTECTIVE MEASURE	STATUS
Management enforces the policy of honoring any copyright/licensing agreement which may apply to proprietary and/or commercially procured software, e.g., WordPerfect, Lotus, etc.	I P AR NA DK
Users understand that Federal government computer systems are to be used for official purposes only and are not to be used for personal or financial gain or for playing games, sending unofficial e-mail, etc.	I P AR NA DK
Access to automated information systems by foreign nationals is requested through the Center Security Office for appropriate investigation and approval prior to granting them access.	I P AR NA DK
All persons, to include contractors, using your system are assigned an ADP Position Sensitivity Level.	I P AR NA DK
Site personnel are informed of how to report known or suspected unauthorized access to the building.	I P AR NA DK
Site personnel are informed of how to report known or suspected unauthorized access to their work area.	I P AR NA DK
Only persons with valid security badges are allowed unescorted access to work areas.	I P AR NA DK
Site personnel are instructed to challenge individuals in their work areas who are not displaying a security badge.	I P AR NA DK
At a minimum, verbal approval from line management is required before anyone is given access to any system included in this assessment.	I P AR NA DK
Line managers identify, in writing, a limited number of persons for each system who are responsible for issuing/maintaining passwords for that system.	I P AR NA DK
Line managers/supervisors annually re-validate the need for persons to use	I P AR NA DK

KEY: I = Implemented; P = Planned; AR = Accepting Risk; NA = Not Applicable; DK = Don't Know

BRANCH REPRESENTATIVE

(Please circle the appropriate status for each measure)

PROTECTIVE MEASURE	STATUS
systems within their organization.	
Line managers have established procedures to insure that system administrators are notified promptly whenever employees (including visiting or guest researchers) no longer require access to their systems.	I P AR NA DK
The organization's policy is to provide all new users with a unique user name and identification number and a temporary, randomly generated, password.	I P AR NA DK
The organization has implemented procedures to insure that only the intended user receives temporary passwords issued for systems within the organization.	I P AR NA DK
Line managers enforce a policy that the number of people given passwords which grant system level privileges is kept to a minimum and that they are identified in writing.	I P AR NA DK
The organization's policy is that passwords must be different from the user name, contain at least six alphanumeric characters, one non-alphanumeric character and no dictionary words.	I P AR NA DK
Procedures are in place to eliminate system access privileges when a remote user terminates employment or changes jobs.	I P AR NA DK
An individual at each off-site location which can access systems included in this assessment is responsible for automated information security at that location.	I P AR NA DK
Phone numbers for dial up access are distributed to identified and authorized users but are not posted or published in a public place	I P AR NA DK
Work areas containing system equipment, including areas under raised floors and above false ceilings, are free from combustible materials, supplies and trash.	I P AR NA DK
Emergency evacuation routes are posted in all work areas.	I P AR NA DK

KEY: I = Implemented; P = Planned; AR = Accepting Risk; NA = Not Applicable; DK = Don't Know

BRANCH REPRESENTATIVE

(Please circle the appropriate status for each measure)

PROTECTIVE MEASURE	STATUS				
Work areas containing system equipment valued at more than $1 million are equipped with appropriate automatic fire suppression systems.	I	P	AR	NA	DK
The local fire department has provided training in the use of Halon, CO2 and water for fire suppression, as appropriate.	I	P	AR	NA	DK
The organization enforces a policy of using system hardware for authorized purposes only.	I	P	AR	NA	DK
A vendor maintenance contract is available for system hardware maintenance support.	I	P	AR	NA	DK
Someone has been assigned responsibility for system hardware maintenance.	I	P	AR	NA	DK
Line management approves all system hardware procurement.	I	P	AR	NA	DK
Security is addressed in the planning phase of any major hardware procurement.	I	P	AR	NA	DK
Someone has been assigned responsibility for system software maintenance.	I	P	AR	NA	DK
Line management approves all software procurement.	I	P	AR	NA	DK
Procedures are in place to effect complete control over changes to the operating system and to insure that the system remains intact until the changes are approved.	I	P	AR	NA	DK
Security is addressed in planning for any major software development or procurement action.	I	P	AR	NA	DK
A property custodian has been assigned responsibility for all system hardware.	I	P	AR	NA	DK
The property custodian is notified prior to employee transfers and terminations.	I	P	AR	NA	DK

KEY: I = Implemented; P = Planned; AR = Accepting Risk; NA = Not Applicable; DK = Don't Know